



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/664,799	09/18/2003	Radia J. Perlman	SMY-263.01 (25087-26301)	3482
45774 7590 04/02/2007 CHAPIN INTELLECTUAL PROPERTY LAW, LLC WESTBOROUGH OFFICE PARK 1700 WEST PARK DRIVE WESTBOROUGH, MA 01581			EXAMINER SMITHERS, MATTHEW	
			ART UNIT 2137	PAPER NUMBER

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/664,799

Applicant(s)

PERLMAN, RADIA J.

Examiner

Matthew B. Smithers

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 September 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 7-17 and 23-25 is/are rejected.
- 7) ☒ Claim(s) 18-22 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 September 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 7/23/04; 4/11/05; 11/23/05.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Information Disclosure Statement

The information disclosure statements filed July 23, 2004, April 11, 2005, and November 23, 2005 have been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Objections

Claim 18 is objected to because of the following informalities: In the second limitation of the claim it appears the word "from" should be "form". Appropriate correction is required.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Art Unit: 2137

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-4 and 14-17 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 20-22 and 31-34 of copending Application No. 10/665386. Although the conflicting claims are not identical, they are not patentably distinct from each other because all the limitations of claims 1-4 and 14-17 of the instant application are anticipated by patent application claims 20-22 and 31-34.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 25 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. With respect to claim 25, the computer readable medium, as described in the specification (see page 13, line 27 to page 14, line 14), can be non-writeable media, writeable media or communications media (i.e. carrier waves). The latter form does not fall within one of the four statutory classes of an invention.

Specifically, the carrier waves lack the necessary physical articles to constitute a machine or a manufacture within the meaning of 101 and the carrier waves are clearly

not a series of steps to a process nor are they a combination of chemical compounds to a composition of matter.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 7-13, 23 and 24 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. 5,638,445 granted to Spelman et al.

Regarding claim 1, Spelman meets the claimed limitations as follows:

"A method for performing blind decryption of a message M, wherein said message is encrypted by a first node using an encryption function to form an encrypted message, the method comprising the steps of:

blinding said encrypted message with a blinding function z to form a blinded and encrypted message, wherein z has an inverse z^{-1} ;" see column 9, lines 28-42 (. . . Party B blinds this encrypted message . . .)

"in a first communicating step, communicating said blinded and encrypted message to a decryption agent;" see column 9, lines 28-42 (. . . Party B . . . sends the blinded and encrypted message to the Decryptor. . .)

"decrypting said blinded and encrypted message by said decryption agent using a decryption function to form a blinded message, wherein said decryption function is the

Art Unit: 2137

inverse of said encryption function;" see column 9, lines 28-42 (. . . The Decryptor uses its private key to decrypt the received message producing a message that is still blinded . . .)

"in a second communicating step, communicating said blinded message to said first node;" see column 9, lines 28-42 (. . . The Decryptor sends this message back to Party B . . .)

"and unblinding said blinded message using $z_{sup.-1}$, to obtain said message M." see column 9, lines 28-42 (. . . unblinds the message and reads it.).

Regarding claim 2, Spelman meets the claimed limitations as follows:

"The method of claim 1 wherein said first node and said decryption agent are communicably coupled via a network, and at least one of said first and second communicating steps comprises the step of communicating the respective message over said network." see column 4, lines 43-58 (. . . In addition the communications media over which the transfers of information take place can also be . . . telephone lines, cable, the Internet, satellite transmissions, or radio transmissions . . .).

Regarding claim 3, Spelman meets the claimed limitations as follows:

"The method of claim 2 wherein said first and second communicating steps comprise communicating the respective messages over said network." see column 4, lines 43-58 (. . . In addition the communications media over which the transfers of information take place can also be . . . telephone lines, cable, the Internet, satellite transmissions, or radio transmissions . . .).

Regarding claim 7, Spelman meets the claimed limitations as follows:

"The method of claim 1 further including the step of generating said message M at said first node." see column 9, lines 28-42.

Regarding claim 8, Spelman meets the claimed limitations as follows:

"The method of claim 1 wherein said encryption and decryption functions are, respectively, public and private keys of a public key pair." see column 6, lines 22-45.

Regarding claim 9, Spelman meets the claimed limitations as follows:

"The method of claim 8 wherein said public and private keys comprise a RSA public/private key pair of the form (e, n) and (d, n) , respectively." see column 6, lines 22-45.

Regarding claim 10, Spelman meets the claimed limitations as follows:

"The method of claim 9 wherein said blinding function, z , is a blinding number R having an inverse R^{-1} that satisfies $R \cdot R^{-1} = 1 \pmod n$ and wherein said blinding step includes the step of forming said blinded and encrypted message as the product $(R^e \cdot M^e \pmod n)$ where $(M^e \pmod n)$ is said message M encrypted using said public encryption key." see column 6, lines 22-45.

Regarding claim 11, Spelman meets the claimed limitations as follows:

"The method of claim 10 wherein the decryption step includes raising the product $((R^e \cdot M^e) \pmod n)$ to the power $d \pmod n$, forming $((R^e \cdot M^e) \pmod n)^d \pmod n$ to form said blinded message $R \cdot M \pmod n$." see column 5, line 66 to column 6, line 13 and column 6, lines 22-45.

Regarding claim 12, Spelman meets the claimed limitations as follows:

Art Unit: 2137

"The method of claim 11 wherein the unblinding step includes unblinding said blinded message $R \cdot M \bmod n$ using $R^{\text{sup.}-1}$ to obtain said message M." see column 5, line 66 to column 6, line 13 and column 6, lines 22-45.

Regarding claim 13, Spelman meets the claimed limitations as follows:

"The method of claim 10 further including the step of generating an integer random number and utilizing said random number as the blinding number R." see column 5, line 66 to column 6, line 13 and column 6, lines 22-45.

Regarding claim 23, Spelman meets the claimed limitations as follows:

"A system for performing blind decryption of a message M comprising: a first node and a decryption agent communicably coupled via a communications network; said first node operative to: encrypt said message using an encryption function to form an encrypted message; blind said encrypted message with a blinding function z to form a blinded and encrypted message, wherein z has an inverse $z^{\text{sup.}-1}$;" see column 9, lines 28-42 (. . . Party B blinds this encrypted message . . .)

"communicate said blinded and encrypted message to a decryption agent" see column 9, lines 28-42 (. . . Party B . . . sends the blinded and encrypted message to the Decryptor. . .)

"decrypt said blinded and encrypted message by said decryption agent using a decryption function to form a blinded message, wherein said decryption function is the inverse of said encryption function;" see column 9, lines 28-42 (. . . The Decryptor uses its private key to decrypt the received message producing a message that is still blinded . . .)

"communicate said blinded message to said first node;" see column 9, lines 28-42 (. . . The Decryptor sends this message back to Party B . . .)

"and unblind said blinded message using $z.\text{sup.}-1$, to obtain said message M." see ;" see column 9, lines 28-42 (. . . unblinds the message and reads it.).

Regarding claim 24, Spelman meets the claimed limitations as follows:

"A system for performing blind decryption of a message M comprising: a first node and a decryption agent communicably coupled via a communications network; means in said first node for: blinding said encrypted message with a blinding function z to form a blinded and encrypted message, wherein z has an inverse $z.\text{sup.}-1$;" see column 9, lines 28-42 (. . . Party B blinds this encrypted message . . .)

"communicating said blinded and encrypted message to a decryption agent;" see column 9, lines 28-42 (. . . Party B . . . sends the blinded and encrypted message to the Decryptor. . .)

"decrypting said blinded and encrypted message by said decryption agent using a decryption function to form a blinded message, wherein said decryption function is the inverse of said encryption function;" see column 9, lines 28-42 (. . . The Decryptor uses its private key to decrypt the received message producing a message that is still blinded . . .)

"communicating said blinded message to said first node;" see column 9, lines 28-42 (. . . The Decryptor sends this message back to Party B . . .)

"and unblinding said blinded message using $z.\text{sup.}-1$, to obtain said message M." see ;" see column 9, lines 28-42 (. . . unblinds the message and reads it.).

Allowable Subject Matter

Claims 5, 6 and 18-22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

With respect to claims 5 and 6, the cited prior art fails to specifically teach the decryption function comprises an ephemeral decryption key and further including the step of rendering said ephemeral decryption key unusable after a predetermined time.

With respect to claims 18-22, the cited prior art fails to specifically teach the further steps of: selecting a blinding number y having an inverse blinding number $y.\sup.-1$; blinding said message M using said blinding number y to form a first blinded message; forwarding said first blinded message to an encryption agent; encrypting, by said encryption agent, said first blinded message to form a first blinded and encrypted message wherein said encryption is performed using said encryption function and wherein said encryption function and said corresponding decryption function are secret encryption and decryption keys, respectively; forwarding said first blinded and encrypted message from said encryption agent to said first node; and unblinding said first blinded and encrypted message using said inverse blinding number $y.\sup.-1$ to form said encrypted message.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Zolotorev et al (US 7,058,808) discloses a method for using blind RSA-signatures.

B. Jakobsson (US 6,049,613) discloses a method for applying blinded values to encrypt data.

C. Puhl et al (US 5,564,106) discloses a method for providing blind access to an encryption key.

D. Chaum (US 4,947,430) discloses a method for checking, blinding and unblinding signatures.

E. Chaum (US 4,914,698) discloses a method for using blind signatures in a commerce system.

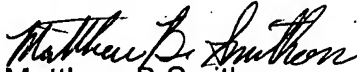
F. Chaum (US 4,759,063) discloses a method for using blind signatures on messages sent from one party to the next party.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


Matthew B Smithers
Primary Examiner
Art Unit 2137